

PROCÉDÉ ET SYSTÈME HAUTEMENT SÉCURISÉS POUR LA DISTRIBUTION
DE FLUX AUDIOVISUELS

La présente invention se rapporte au domaine de la
distribution très sécurisée de séquences audiovisuelles
numériques.

On se propose dans la présente invention de fournir un
procédé et un système permettant de protéger visuellement
et/ou auditivement une séquence audiovisuelle numérique
issue d'un standard de compression numérique ou d'une norme
de compression numérique, de distribuer de manière hautement
sécurisée ladite séquence à travers un réseau de
télécommunication et de reconstituer son contenu original à
partir d'un flux audiovisuel protégé sur un module de
recomposition de l'équipement destinataire.

État de la technique

On connaît dans l'état de la technique le brevet
américain US6351538 ayant pour titre "CONDITIONAL ACCES AND
COPY PROTECTION SCHEME FOR MPEG ENCODED VIDEO DATA".

Ce document concerne la protection d'un flux vidéo
numérique. La protection est appliquée lorsque le flux vidéo
est en cours de numérisation. Le flux vidéo numérique est
considéré comme composé d'un flux d'images vidéo codées par
compensation de mouvement et d'un second flux d'image vidéo
dites de référence, servant à la prédiction de mouvement.
Selon ce document de l'art antérieur, on chiffre le flux
d'images vidéo de référence, la quantité de données à
chiffrer pour protéger le flux est donc réduit. Les
paramètres qui ont permis de réaliser cette opération de
chiffrement sont stockés dans le flux vidéo numérique dans
une partie réservée à cet effet. Le chiffrement des images
de référence est suffisant pour protéger le contenu du flux
vidéo numérique car le reste du flux vidéo numérique est
composé d'image vidéo codée par compensation de mouvement à

partir du flux d'images vidéo de référence. Une double opération de chiffrement est réalisée, un chiffrement des images de référence par une première fonction de chiffrement simple (application d'un XOR ou exclusif) puis chiffrement
5 complexe des paramètres de la première fonction par une seconde fonction de chiffrement plus complexe. Ce double chiffrement permet de concentrer la protection sur une quantité de données encore moindre que la quantité que représentent les images de référence. Le flux d'images vidéo
10 codées par compensation de mouvement et le flux d'images vidéo de référence (alors protégé) sont ensuite multiplexés pour former le flux vidéo compressé protégé.

Cette solution ne prévoit pas une séparation en deux flux. Elle décrit une décomposition en deux sous ensembles,
15 composée d'une part d'images vidéo de référence et d'images vidéo obtenues par compensation de mouvement, hors notre invention réalise une séparation physique du flux vidéo en deux flux, un flux principal modifié qui est alors un flux vidéo compressé auto-protégé et un flux complémentaire.

20 Le but de la présente invention est de conserver le format du flux vidéo numérique et opérer la protection à posteriori à la compression, ce qui n'est pas le cas de l'invention du document de l'art antérieur où il est cité clairement que la protection est faite pendant l'encodage du
25 flux vidéo.

Enfin aucune analyse du flux numérique original n'est réalisée, pour en analyser la conformité des données par conséquent l'invention du document D'est susceptible de rendre le flux vidéo numérique protégé non conforme au
30 standard duquel il est issu.

L'art antérieur comprend également le brevet international WO 03/007608 dont le titre est "MOTION PICTURE ENCRYPTION METHOD AND APPARATUS WITH VARIABLE SECURITY ».

Selon ce document de l'art antérieur, la protection d'un flux vidéo numérique est réalisée par une méthode de chiffrement à niveau de sécurité variable.

Le flux vidéo compressé est divisé en blocs de taille fixe. La protection s'effectue sur ces blocs de données numériques. La protection est effectuée tour à tour sur chaque bloc. Seuls quelques octets sont chiffrés dans chaque bloc, le reste du bloc reste inchangé. Le choix des octets à protéger est obtenu par l'intermédiaire d'un générateur pseudo aléatoire où par l'intermédiaire d'une « look up table », l'octet sélectionné peut aussi être chiffré en utilisant une « look up table ».

Selon ce document de l'art antérieur, seuls trois pour cent de chaque bloc doivent être chiffrés pour obtenir une dégradation du flux numérique compressé satisfaisante le rendant illisible pour un appareil de rendu standard.

Cette solution de l'art antérieur ne réalise pas une séparation en deux flux vidéo compressé, comme le fait notre invention, mais réalise sa décomposition en blocs de taille fixe qui sont traités indépendamment pour chiffrer quelques données de chaque bloc. Le but de cette opération de chiffrement est de rendre le flux vidéo compressé illisible pour un décodeur standard, par conséquent l'invention du document D2 est fondamentalement différente de notre invention qui opère une opération de protection tout en gardant le flux conforme au format d'origine, c'est-à-dire lisible par un décodeur standard.

Objet de l'invention

La présente invention se rapporte plus particulièrement à un dispositif capable de transmettre de façon sécurisée à travers un réseau de télécommunication, un ensemble de flux audiovisuels de haute qualité vers un écran de visualisation et/ou vers une sortie audio appartenant à un terminal ou à un dispositif d'affichage, tel qu'un écran

de télévision, un ordinateur ou encore un téléphone mobile, un terminal mobile de type PDA (Personal Digital Assistant), ou autre, tout en préservant la qualité audiovisuelle mais en évitant toute utilisation frauduleuse comme la
5 possibilité de faire des copies pirates des contenus diffusés.

Avantageusement, l'invention se réfère à un procédé et un système client-serveur qui protège les contenus audiovisuels en les séparant en deux parties, la deuxième
10 partie étant absolument indispensable pour la reconstitution du flux original, ce dernier étant restitué en fonction de la recombinaison de la première partie avec la deuxième partie

Le procédé utilisé dans la présente invention pour la
15 description d'un exemple préféré mais non limitatif de réalisation, sépare le flux audiovisuel en deux parties, de manière à ce que la première partie appelée « flux principal modifié » contienne la quasi-totalité de l'information initiale, par exemple plus de 99%, et une deuxième partie
20 appelée « information complémentaire » contenant des éléments ciblés de l'information originale, qui est de très petite taille par rapport à la première partie.

Actuellement, il est possible de transmettre des programmes audiovisuels sous forme numérique via des réseaux
25 de diffusion de type hertzien, câble, satellite, etc. ou via des réseaux de télécommunication type DSL (Digital Subscriber Line) ou BLR (Boucle Locale Radio) ou via des réseaux DAB (Digital Audio Broadcasting), ainsi que via tout réseau de télécommunication sans fil de type GSM, GPRS,
30 EDGE, UMTS, Bluetooth, Wifi, etc. Par ailleurs, pour éviter le piratage des œuvres ainsi diffusées, ces dernières sont souvent cryptées ou brouillées par divers moyens bien connus par l'art antérieur.

On connaît également dans l'art antérieur du domaine du
35 cryptage l'article écrit par Zeng W. et al., publié dans ACM

Multimedia Proceedings of the International Conference en octobre 1999 et intitulé « Efficient Frequency Domain Video Scrambling for Content Access Control ». Dans cet article, les auteurs décrivent une méthode de protection de données numériques codant un contenu multimédia. La méthode repose sur des générateurs pseudo-aléatoires pour générer trois opérations pseudo-aléatoires de base (inversion de bit, permutation et rotation de bloc de coefficients) pouvant être combinées et contrôlées par des clés de cryptage. Dans cet art antérieur, l'ensemble des données originales sont présentes dans le flux protégé et l'accès au contenu original est entièrement conditionné par la possession ou non de clés de cryptage. Cette solution n'utilise pas cependant différentes modélisations de générateurs pseudo-aléatoires, ni de données du flux original comme clé cryptographique. Étant donné que toutes les données originales du flux reste à l'intérieur du flux protégé, cet art antérieur représente une solution de cryptage classique, et par conséquent ne correspond pas aux objectifs de haute sécurité, objet de la présente invention.

Concernant la séparation d'un flux audiovisuel en deux parties dans le but de le protéger, l'art antérieur connaît l'article « Protecting VoD the Easier Way », Griwodz et al., Proceedings of the ACM Multimedia, septembre 1998, dans lequel les auteurs décrivent un procédé de distribution, via des réseaux larges bandes ou des serveurs temporaires et une connexion point à point sécurisée, de contenus multimédia protégés dont l'accès est contrôlé et tracé. Le flux audiovisuel original est délibérément corrompu par une modification prédéterminée de certains octets au sein du flux, sans aucune analyse de la structure et du contenu du flux, donc sans tenir compte de la conformité avec le format natif, lesdits octets étant choisis selon une loi prédéfinie (loi de Poisson). Un signal permettant la reconstruction est transmis ultérieurement au client au moment de la

visualisation du contenu : une clé est d'abord communiquée au client qui lui permettra de recalculer l'emplacement des octets corrompus au sein du flux. Puis un signal contenant les octets originaux lui est envoyé après cryptage afin de
5 reconstruire le flux initial. La reconstruction du flux est ainsi conditionnée par une simple clé et par conséquent le procédé décrit dans ce document de l'art antérieur n'apporte pas le haut niveau de sécurité proposé dans la présente invention.

10

La présente invention concerne des modélisations de processus pseudo-aléatoires utilisés pour définir à quel endroit et quelle modification sera appliquée, lesdites modélisations étant un modèle mathématique décrivant un
15 phénomène naturel aléatoire. Ces processus pseudo-aléatoires sont initialisés par différentes graines, le processus aléatoire générant les graines est également modifié dynamiquement par un ensemble de paramètres relatifs à sa modélisation durant la génération de la séquence pseudo-
20 aléatoire.

Avantageusement, lesdites graines d'initialisation et lesdits paramètres de modélisation sont les données extraites du flux original. Avantageusement, la protection appliquée aux contenus distribués par le système sécurisé
25 dans la présente invention, est basée sur le principe de suppression et de remplacement de certaines informations présentes dans le signal audiovisuel original encodé, par une méthode quelconque, soit : substitution, modification, permutation ou déplacement de l'information. Cette
30 protection est également basée sur la connaissance de la structure du flux numérique. La solution consiste à extraire et à conserver en permanence dans un serveur sécurisé lié au réseau de diffusion et de transmission, dans ladite information complémentaire, une partie des données du
35 programme audiovisuel enregistré chez l'utilisateur ou

diffusé en direct, cette partie étant primordiale pour reconstituer ledit programme audiovisuel sur un écran ou sur une sortie audio d'un terminal, mais étant d'un volume très faible par rapport au volume total du programme audiovisuel numérique enregistré chez l'utilisateur ou reçu en temps réel par l'utilisateur. La partie manquante (l'information complémentaire) sera transmise via le réseau sécurisé avantageusement réparti, de diffusion ou de transmission, au moment de la visualisation et/ou de l'audition dudit programme audiovisuel. Avantageusement, les données enlevées dans le programme audiovisuel original sont substituées, pour former le flux principal modifié, par des données aléatoires ou calculées, appelées leurres.

Le fait d'avoir enlevé et substitué par des leurres une partie des données originales du flux audiovisuel original lors de la génération du flux principal modifié, ne permet pas la restitution dudit flux original à partir des seules données dudit flux principal modifié. Dans un mode de mise en œuvre, ledit flux principal modifié est entièrement compatible avec le format du flux d'origine, et peut donc être copié et lu par un lecteur standard, mais il est complètement incohérent de point de vue perception visuelle et auditive humaine. Dans un autre mode de mise en œuvre, ledit flux principal modifié est de format quelconque.

Le flux numérique étant séparé en deux parties, la plus grande partie, ledit flux principal modifié, sera donc transmise via un réseau de diffusion classique, alors que la partie manquante, ladite information complémentaire, sera envoyée à la demande via un réseau de télécommunication bande étroite comme les réseaux téléphoniques classiques ou les réseaux cellulaires de type GSM, GPRS, EDGE ou UMTS ou en utilisant une petite partie d'un réseau de type DSL ou BLR, ou en utilisant un sous-ensemble de la bande passante partagée sur un réseau câblé, ou encore via un support physique comme une carte à mémoire ou tout autre support.

Dans un mode de réalisation particulier, les deux réseaux peuvent être confondus, tout en gardant les deux voies de transmission séparées. Le flux audiovisuel est reconstitué sur l'équipement destinataire par un module de synthèse à partir du flux principal modifié et de l'information complémentaire, envoyée pièce par pièce pendant la consommation du flux audiovisuel.

Le fait que l'information complémentaire représente une toute petite partie du flux original, par exemple seulement 1%, permet son envoi à travers des réseaux à faible débit. De préférence, lorsque le flux principal modifié est déjà téléchargé sur le disque dur de l'équipement destinataire, l'information complémentaire est envoyée par un réseau bande étroite. Une information complémentaire de faible taille facilite sa distribution sur tout type de réseau et contribue au renforcement de la sécurité.

L'objet de la présente invention concerne un module d'analyse qui met en œuvre un procédé de sécurisation, de manière à optimiser la structure et le contenu de l'information complémentaire à l'aide de différents algorithmes et modélisations, dans le but de minimiser la taille de ladite information complémentaire et de renforcer la sécurité.

La présente invention concerne dans son acception la plus générale, un procédé pour la distribution de séquences audiovisuelles selon un format de flux original constitué par une succession de trames, ledit flux original sur lequel on procède, avant la transmission à l'équipement client, à une analyse pour générer un premier flux principal modifié et une information complémentaire, puis à transmettre par voie séparée, le flux principal modifié et l'information complémentaire vers l'équipement destinataire, et pour lequel on calcule sur l'équipement destinataire une synthèse d'un flux au format original en fonction dudit flux

principal modifié et de ladite information complémentaire, ladite analyse du flux original étant constituée :

- d'une étape d'application d'opérations comprenant des modélisations, générant des séquences de valeurs pseudo-aléatoires à paramètres connus,

- d'une étape d'extraction des données originales en fonction desdites séquences pseudo-aléatoires, et

- d'une étape de stockage desdits paramètres desdites modélisations dans l'information complémentaire.

Selon un mode de mise en œuvre, lesdits paramètres sont stockés intégralement dans l'information complémentaire.

Selon un autre mode de mise œuvre, lesdits paramètres sont stockés partiellement dans l'information complémentaire.

Avantageusement, lesdites valeurs pseudo-aléatoires représentent des informations relatives à au moins une caractéristique des données extraites dans le flux d'origine.

Avantageusement, lesdites valeurs pseudo-aléatoires représentent des informations relatives à la position de la donnée extraite dans le flux d'origine.

De plus, lesdits paramètres desdites modélisations sont aléatoires.

Selon une variante, lesdits paramètres desdites modélisations sont des données extraites du flux d'origine.

Selon une autre variante, lesdites modélisations sont aléatoires.

Avantageusement, lesdites modélisations sont générées à partir d'au moins une caractéristique propre à l'équipement d'analyse.

Avantageusement, lesdites modélisations sont stockées dans l'équipement d'analyse.

Dans un mode de réalisation, lesdites modélisations utilisées par l'équipement d'analyse sont envoyées au préalable par l'équipement destinataire.

5 Dans un autre mode de réalisation, lesdites modélisations sont stockées dans une carte à puce de l'équipement destinataire.

De préférence, ladite synthèse du flux d'origine est effectuée en fonctions des paramètres des modélisations, reproduisant les valeurs pseudo-aléatoires obtenues lors des
10 étapes d'analyse.

De plus, le procédé est sans perte.

La présente invention concerne également un système pour la mise en œuvre du procédé, comportant au moins un serveur multimédia contenant les séquences audiovisuelles
15 originales, comportant un dispositif d'analyse du flux audiovisuel pour la séparation du flux vidéo original en un flux principal modifié et en une information complémentaire en fonction de ladite analyse, au moins un réseau de télécommunication pour la transmission et au moins un
20 dispositif sur l'équipement destinataire pour la reconstruction du flux audiovisuel en fonction dudit flux principal modifié et de ladite information complémentaire.

La présente invention sera mieux comprise à l'aide des exemples de réalisation et des étapes détaillées ci-après.
25 L'information complémentaire représente l'ensemble des données et informations nécessaires à la reconstruction du flux original. Avantageusement, elle contient les valeurs originales extraites, leurs positions et des informations nécessaires à la reconstruction, qui sont relatives aux
30 caractéristiques desdites données originales du flux. Néanmoins, dans ce cas, les informations de position des données originales ont une taille de l'ordre de 50% de l'information complémentaire. Une compression de l'information complémentaire s'avère inefficace, en raison

du fait que les informations de position sont statistiquement indépendantes et donc de faible redondance. De plus, la présence des informations de position volumineuses limite d'autant la sécurité, car ce sont
5 autant de données originales qui ne sont pas extraites, substituées par des leurres et stockés dans l'information complémentaire.

Avantageusement, on se propose dans la présente invention de réduire le nombre des informations contenues
10 dans l'information complémentaire concernant les données originales, et de les définir à l'aide de modélisations. De cette façon, ces informations sont reproduites lors de la reconstitution du flux original, les modélisations et leurs paramètres étant connus.

15 Un exemple de réalisation préféré, mais non limitatif décrit dans la présente invention concerne des modélisations et des algorithmes de générateurs de séquences pseudo-aléatoires, initialisés par des processus aléatoires.

Un processus aléatoire est un signal par exemple
20 temporel $s(t)$ dont on ne peut prévoir la valeur à l'avance quel que soit l'instant considéré. Un tel processus est généré soit en utilisant des phénomènes physiques imprévisibles (comme les phénomènes de dégradation des atomes des éléments radioactifs) ou soit en utilisant des
25 processus pseudo-aléatoires couplés avec des facteurs aléatoires (comme un algorithme de type « Roue de la fortune »). Fort complexes (dépendant de phénomènes non toujours maîtrisés par l'homme de l'art) et avec des contraintes de temps d'exécution trop grands sur un
30 ordinateur, les processus aléatoires sont en général utilisés en combinaison avec des processus pseudo-aléatoires. Les générateurs aléatoires sont utilisés pour la

modélisation et l'initialisation des générateurs pseudo-aléatoires.

Un processus pseudo-aléatoire est un processus déterministe qui permet de générer une séquence de nombres
 5 qui possède une distribution choisie de façon plus ou moins uniforme. Ces processus sont initialisés par une graine qui sert de point de départ à la séquence. L'avantage des processus pseudo-aléatoires est qu'ils sont rapides (temps d'exécution court pour un ordinateur), car issus de calculs
 10 mathématiques peu complexes. La qualité d'un générateur pseudo-aléatoire se mesure en fonction de sa période (nombre de valeurs minimales que contient la séquence avant de se reproduire à l'identique) et de l'équidistribution qu'il va fournir dans plusieurs directions. Un générateur pseudo-
 15 aléatoire performant possède une période longue et une équidistribution dans un grand nombre de directions.

Un exemple de générateur de nombres pseudo-aléatoire (générateur pseudo-aléatoire linéaire congruent) est décrit par l'expression suivante, S_n étant le terme de
 20 la suite, $M-1$ la valeur maximale pour le terme S_n , A et B étant respectivement la pente et l'ordonnée à l'origine d'une droite F d'équation :

$$S_{n+1} = (S_n * A + B) \bmod(M)$$

Le terme S_n représente dans notre cas la graine mise à
 25 jour comme il suit :

```
graine = (graine * 0x5DEECE66DL + 0xBL) &
((1L << 48) - 1);
Sn = graine
A = 0x5DEECE66DL
30 B = 0xBL
mod(M) = & ((1L << 48) - 1);
```

Ce générateur pseudo-aléatoire possède une période théorique
 35 de 2^{48} , l'opération $\& ((1L \ll 48) - 1)$ assure la

périodicité en rejetant toute valeur supérieure à 2^{48} . Le multiplicateur A est choisi de telle sorte qu'une oscillation soit obtenue rapidement.

5 Un exemple de générateur pseudo-aléatoire est illustré sur la figure 1.

Des valeurs successives sont générées à partir de la graine S_0 posée en abscisse. L'ordonnée correspondante à la projection de S_0 sur la droite F de pente A donne en ordonnée la valeur de la graine suivante S_1 , dont la valeur
10 posée en abscisse et projetée à partir de la droite F en ordonnée, donnera la valeur de la future graine S_2 , et ainsi cette opération itérative produit une séquence de graines.

Lorsque la graine est supérieure ou égale à la valeur $S_{\max} = (M-B)/A$, le reste de la division entière (la fonction
15 « modulo ») de la valeur générée pour S_{\max} divisée par M est renvoyé au générateur pour continuer la séquence, résultat de la congruence de la fonction modulo.

Des exemples de réalisation sont décrits par la suite, mettant en oeuvre des modélisations de fonctions linéaires
20 congruentes produisant des valeurs pseudo-aléatoires, qui sont utilisées lors de l'analyse et la synthèse.

Avantageusement, l'analyse effectuée dans le but de séparer le flux original en un flux principal modifié et une information complémentaire utilise un grand nombre de
25 modélisations de processus pseudo-aléatoires afin de garantir un maximum d'aléa et d'apporter ainsi une sécurité élevée. Ladite analyse est constituée des étapes suivantes :

- d'une étape d'application d'opérations comprenant des modélisations de processus pseudo-aléatoires, générant des séquences de valeurs pseudo-aléatoires à
30 paramètres connus,
- d'une étape d'extraction des données originales en fonction desdites séquences pseudo-aléatoires,
- d'une étape d'introduction des données leurres
35 à la place des données originales extraites,

• d'une étape de stockage desdits paramètres desdites modélisations dans l'information complémentaire.

Le procédé de protection pour chacun des formats numériques différents possède son propre algorithme d'analyse constitué des étapes énumérées et garantissant une dégradation audiovisuelle. Incluant des processus pseudo-aléatoires, ladite analyse assure l'unicité et l'efficacité de la protection. C'est à ce moment du processus qu'on définit le degré de sécurité introduite dans un flux, à partir des combinaisons possibles générées par le processus pseudo-aléatoire. Avantageusement, les séquences pseudo-aléatoires générées lors de l'analyse sont utilisées pour :

- Choisir la position d'une donnée à extraire,
- Choisir le nombre de données à extraire pour une portion de flux donnée,
- Choisir la taille de la portion de flux à protéger,
- Choisir le nombre de portion à protéger,
- Choisir les leurres et les insérer à la place des données originales.

Concernant l'évaluation du degré de sécurité introduite, on prendra comme référence de l'art antérieur le procédé de protection par cryptage AES (« Asymmetric Encryption System »), la clé ayant une longueur de 128 bits, le nombre de combinaisons possible est alors :

$2^{128} = 3,40 \times 10^{38}$ possibilités de clé de 128 bits

Dans la présente invention, on émet l'hypothèse que tous les événements sont aléatoires, on prend une portion de flux de longueur 300 octets, dans lesquels on ajoute « n » = 5 leurres par exemple, chacun des leurres ayant une longueur de 1 octet. On arrive au résultat suivant : soit on tient compte de toutes les combinaisons de 5 octets parmi 300 ce qui fait $1,96 \times 10^{10}$ possibilités sachant qu'il y a 2^{40} mots binaires soit $1,10 \times 10^{12}$ mots possibles, et on obtient finalement un total de $2,37 \times 10^{34}$ possibilités. On a supposé connaître le nombre de leurres pour réaliser ce calcul, à

savoir 5 leurres pour une portion de 300 octets. Dans le cas où on ne connaîtrait pas la valeur de « n », on obtient le nombre total des possibilités en sommant le résultat pour chacun des « n » de 1 à 300, ce qui produit un nombre de possibilités considérablement augmenté, avec 300 leurres il y a une combinaison de 300 octets parmi 300 et 2^{2400} mots binaires possibles, donc plus n (le nombre de leurres) est grand plus le nombre de possibilités augmente. Cependant, l'hypothèse précédente considère que tous les tirages sont aléatoires, hors dans un cas réel d'algorithme d'analyse, les séquences générées sont pseudo-aléatoires, donc une personne mal intentionnée pourrait décider de rechercher la graine à partir de laquelle a été générée la séquence pseudo-aléatoire. Sachant que les positions ont été générées par une graine de 32 bits sur un intervalle de 300 valeurs, on obtient alors $2^{32} \times 256^5 = 4,73e+21$ possibilités pour retrouver les valeurs des positions des leurres (pour une graine de 64 bits, on obtient $2,10e+31$ possibilités, et également il faut effectuer la somme de 1 à 300 pour chaque « n » possible dans la portion décrite). En conclusion, il est plus facile pour une personne mal intentionnée d'effectuer la recherche de la graine qu'une recherche exhaustive des positions des leurres à partir du flux protégé. Cependant, lorsqu'une graine codée sur 128 bits est choisie, le nombre de possibilités pour la graine est identique au nombre de clés possible pour la méthode AES avec une clé codée sur 128 bits.

Étant donné qu'un algorithme ne peut être composé uniquement de processus aléatoires pour une question de rapidité d'exécution, l'utilisation de générateur pseudo-aléatoire s'impose, en utilisant pour ce générateur une graine aléatoire qui permettra de fixer le niveau de sécurité souhaité, par exemple choisir une graine de longueur 128 bits. De même, un choix judicieux des paramètres A, B, M et S_0 est effectué de manière à générer

des séquences pseudo-aléatoires avec différents types de distribution.

Dans ce cas, un critère d'évaluation de la sécurité est le nombre de graines nécessaires au processus et la manière dont sont générées les séquences.

Avantageusement, les paramètres A, B, M et S_0 pour la modélisation du générateur sont choisis aléatoirement et restent inchangés pour une portion de flux donné, par exemple pour N octets consécutifs. À la fin de cette portion, les paramètres A, B, M et S_0 sont modifiés, donc choisis à nouveau de manière aléatoire. De cette façon, le jeu des paramètres de modélisation A, B, M et S_0 est changé tous les N octets, avantageusement N lui-même est aléatoire. De préférence, le jeu des paramètres de modélisation A, B, M et S_0 est changé à chaque fois que la valeur S_{\max} est dépassée.

Concernant la recomposition du flux original lors de la synthèse sur l'équipement destinataire, il est indispensable de récupérer les valeurs originales des données extraites du flux original et leurs emplacements au sein du flux. Toutefois, stocker les vraies valeurs et leurs emplacements dans l'information complémentaire produit une information complémentaire, contenant beaucoup de données pouvant être recalculées à partir des paramètres des modélisations utilisés lors de l'analyse. Par conséquent, une optimisation de la taille de l'information complémentaire est effectuée en stockant à l'intérieur uniquement les données originales extraites et des paramètres des modélisations à partir desquels on reproduit les positions et autres caractéristiques des données originales lors de la synthèse sur l'équipement destinataire. Par conséquent, les données relatives aux positions originales étant de l'ordre de 50% de l'information complémentaire, la taille de l'information complémentaire est fortement réduite, tout en assurant la

dégradation audiovisuelle et en augmentant la sécurité, car donnant la possibilité d'extraire plus de données originales et d'introduire plus de leurres.

5 Dans un autre mode de réalisation, les données originales sont extraites sans introduction de leurres à leurs places.

10 L'analyse déterminant les caractéristiques des données à extraire est effectuée en tenant compte des trois contraintes :

- la dégradation du contenu,
- la sécurité,
- le débit de l'information complémentaire.

15 La relation entre ces trois contraintes étant très complexe, on se propose de réduire la taille de l'information complémentaire sans toutefois diminuer la sécurité et la dégradation audiovisuelle.

20 La figure 2 représente l'information complémentaire contenant les valeurs générées par des modélisations à savoir les positions P (figure 2a) et les données originales extraites D. La figure 2b représente l'information complémentaire contenant les paramètres des modélisations S et les données originales extraites D.

25 De préférence, l'information complémentaire contient des données originales D. À la place des positions P, on sauvegarde les paramètres des modélisations ou les graines S à partir desquelles sont générées ces positions. Avantageusement, les graines sont les données extraites du flux original, garantissant ainsi un aléa fort, ou une
30 combinaison de ces données, ce qui entraîne une augmentation de la complexité du chaînage entre graines. Par exemple, pour la première position une graine est tirée en utilisant un processus aléatoire et on réalise pour la deuxième position de donnée à extraire, une seconde graine
35 combinaison de la première graine avec la valeur de la

donnée extraite, et ainsi de suite. Cette opération garantit pour chaque processus pseudo-aléatoire une réinitialisation aléatoire du générateur (la valeur extraite étant aléatoire). Afin d'éviter qu'une portion du flux protégé
5 soit compromise, dans le cas où la première graine serait trouvée, on choisit une graine de 64 bits ou 128 bits générée par un vrai processus aléatoire. Dans ce cas, il s'avère difficile de reconstituer les positions originales, étant donné que les positions sont modélisées à partir de la
10 graine en combinaison avec les valeurs des données originales du flux.

Le contenu original du flux est restitué à partir de la valeur S de la graine ou les paramètres du modèle et les données originales contenues dans l'information
15 complémentaire, par le module de synthèse qui va reconstruire le flux original sur l'équipement destinataire.

De préférence, l'information complémentaire est spécifique à l'équipement d'analyse qui la génère, à l'aide de caractéristiques propres à cet équipement. Par
20 conséquent, l'information complémentaire sera diffusée librement, car elle est interprétable uniquement par cet équipement d'analyse ou par un autre équipement d'analyse possédant exactement les mêmes caractéristiques. Avantageusement, le générateur pseudo-aléatoire possède une
25 modélisation propre à l'équipement d'analyse et/ou relative à au moins une caractéristique propre de l'équipement d'analyse. Dans une réalisation, lesdites modélisations sont stockées dans l'équipement d'analyse. Dans une autre réalisation, lesdites modélisations sont stockées dans
30 l'équipement destinataire. Avantageusement, lesdites modélisations sont stockées dans une carte à puce de l'équipement destinataire. De préférence, lesdites modélisations de l'équipement destinataire sont envoyées à l'équipement d'analyse pour la génération d'une information
35 complémentaire personnalisée pour l'équipement destinataire.

La figure 3 présente un schéma avec une description à titre purement explicatif, d'un mode de réalisation préféré et non limitatif, particulier à système client-serveur pour la mise en œuvre du procédé selon l'invention.

5 Le flux numérique audiovisuel original (1) que l'on souhaite sécuriser est passé via la liaison (2) à un module d'analyse et de protection (31), qui génère un flux principal modifié (32), au format avantageusement identique au format du flux d'entrée (1), en dehors de ce que
10 certaines des données originales ont été remplacées par des valeurs différentes de celles d'origine, et est stocké sur le serveur (3). L'information complémentaire (33), de format quelconque, contient les valeurs des données originales et les paramètres des modélisations, relatives aux
15 caractéristiques des données originales modifiées, remplacées, substituées ou déplacées. Ladite information complémentaire (33) est également stockée sur le serveur (3).

20 Le flux principal modifié (32) est ensuite transmis, via un réseau haut débit (5) de type hertzien, câble, satellite, ou autre, au terminal de l'utilisateur (8), et est stocké dans une mémoire (81) qui peut être par exemple un disque dur. Lorsque l'utilisateur (8) fait la demande de visionnage de la séquence audiovisuelle présente dans sa
25 mémoire (81), deux éventualités sont possibles : dans un premier cas, l'utilisateur (8) ne possède pas tous les droits nécessaires pour voir le flux audiovisuel et dans ce cas, le flux audiovisuel (32) généré par le module d'analyse (31) présent dans sa mémoire (81) est passé au
30 système de synthèse (86), via une mémoire-tampon de lecture (83), qui ne le modifie pas et le transmet à l'identique à un lecteur capable de le décoder (87) et son contenu, dégradé visuellement et/ou auditivement par le module d'embrouillage (31), est affiché sur l'écran de
35 visualisation (9).

Dans un second cas, le serveur (3) décide que l'utilisateur (8) possède les droits pour voir le flux audiovisuel. Dans ce cas, le module de synthèse (86) fait une demande de visionnage au serveur (3) contenant
5 l'information complémentaire (33), nécessaire à la recomposition de la séquence originale (1). Le serveur (3) envoie alors via des réseaux de télécommunication de type ligne téléphonique analogique ou numérique, DSL (« Digital Subscriber Line ») ou BLR (Boucle Locale Radio), via des
10 réseaux DAB (« Digital Audio Broadcasting ») ou via des réseaux de télécommunications mobiles numériques (GSM, GPRS, UMTS) (7) l'information complémentaire (33), permettant la reconstitution du flux audiovisuel original, de façon à ce que l'utilisateur (8) puisse le stocker dans une mémoire-
15 tampon (85). Avantageusement, le réseau (7) peut être du même type que le réseau (5).

Avantageusement, le réseau (7) peut être confondu avec le réseau (5).

Le module de synthèse (86) procède alors à la
20 recomposition du flux audiovisuel original à partir du flux principal modifié qu'il lit dans sa mémoire-tampon de lecture (83) et de l'information complémentaire lue dans la mémoire-tampon (85) qui lui permet de connaître les positions ainsi que les valeurs d'origine des données
25 modifiées. Le flux audiovisuel reconstitué au format original est envoyé à un lecteur-décodeur (87) correspondant à ce format. Le flux audiovisuel original reconstitué est alors affiché sur l'écran de visualisation (9) de l'utilisateur (8).

30 Avantageusement, le flux principal modifié (32) est passé directement via un réseau (5) à la mémoire-tampon de lecture (83) puis au module de synthèse (86).

Avantageusement, le flux principal modifié (32) est inscrit (enregistré) sur un support physique comme un disque
35 de type CD-ROM, un DVD, un disque dur ou une carte à mémoire

(4) . Le flux principal modifié (32) sera ensuite lu depuis le support physique (4) par le lecteur (82) du boîtier (8) pour être transmis à la mémoire-tampon de lecture (83) puis au module de synthèse (86).

5 Avantageusement, l'information complémentaire (33) est enregistrée sur un support physique (6) de format carte de crédit, constitué par une carte à puce ou une carte mémoire flash. Cette carte (6) sera lue par le lecteur de cartes (84) du dispositif de l'utilisateur (8).

10 Avantageusement, la carte (6) contient les algorithmes et les modélisations du générateur de séquences pseudo-aléatoires qui seront exécutés par le système de synthèse (86).

15 Avantageusement, le dispositif (8) est un système autonome, portable et mobile.

REVENDICATIONS

1. Procédé pour la distribution de séquences audiovisuelles selon un format de flux original constitué
5 par une succession de trames, ledit flux original sur lequel on procède, avant la transmission à l'équipement client, à une analyse pour générer un premier flux principal modifié et une information complémentaire, puis à transmettre par
10 voie séparée, le flux principal modifié et l'information complémentaire vers l'équipement destinataire, et pour lequel on calcule sur l'équipement destinataire une synthèse d'un flux au format original en fonction dudit flux principal modifié et de ladite information complémentaire, caractérisé en ce que ladite analyse du flux original est
15 constituée :

- d'une étape d'application d'opérations comprenant des modélisations, générant des séquences de valeurs pseudo-aléatoires à paramètres connus,
- d'une étape d'extraction des données originales en
20 fonction desdites séquences pseudo-aléatoires,
- d'une étape de stockage desdits paramètres desdites modélisations dans l'information complémentaire.

2. Procédé pour la distribution de séquences
25 audiovisuelles selon la revendication 1, caractérisé en ce que lesdits paramètres sont stockés intégralement dans l'information complémentaire.

3. Procédé pour la distribution de séquences
30 audiovisuelles selon la revendication 1, caractérisé en ce que lesdits paramètres sont stockés partiellement dans l'information complémentaire.

4. Procédé pour la distribution de séquences
35 audiovisuelles selon la revendication 1, caractérisé en ce

que lesdites valeurs pseudo-aléatoires représentent des informations relatives à au moins une caractéristique des données extraites dans le flux d'origine.

5 5. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes, caractérisé en ce que lesdites valeurs pseudo-aléatoires représentent des informations relatives à la position de la donnée extraite dans le flux d'origine.

10 6. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes, caractérisé en ce que lesdits paramètres desdites modélisations sont aléatoires.

15 7. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes, caractérisé en ce que lesdits paramètres desdites modélisations sont des données extraites du flux d'origine.

20 8. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes, caractérisé en ce que lesdites modélisations sont aléatoires.

25 9. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes, caractérisé en ce que lesdites modélisations sont générées à partir d'au moins une caractéristique propre à l'équipement
30 d'analyse.

35 10. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes, caractérisé en ce que lesdites modélisations sont stockées dans l'équipement d'analyse.

11. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes, caractérisé en ce que lesdites modélisations utilisées par
5 l'équipement d'analyse sont envoyées au préalable par l'équipement destinataire.

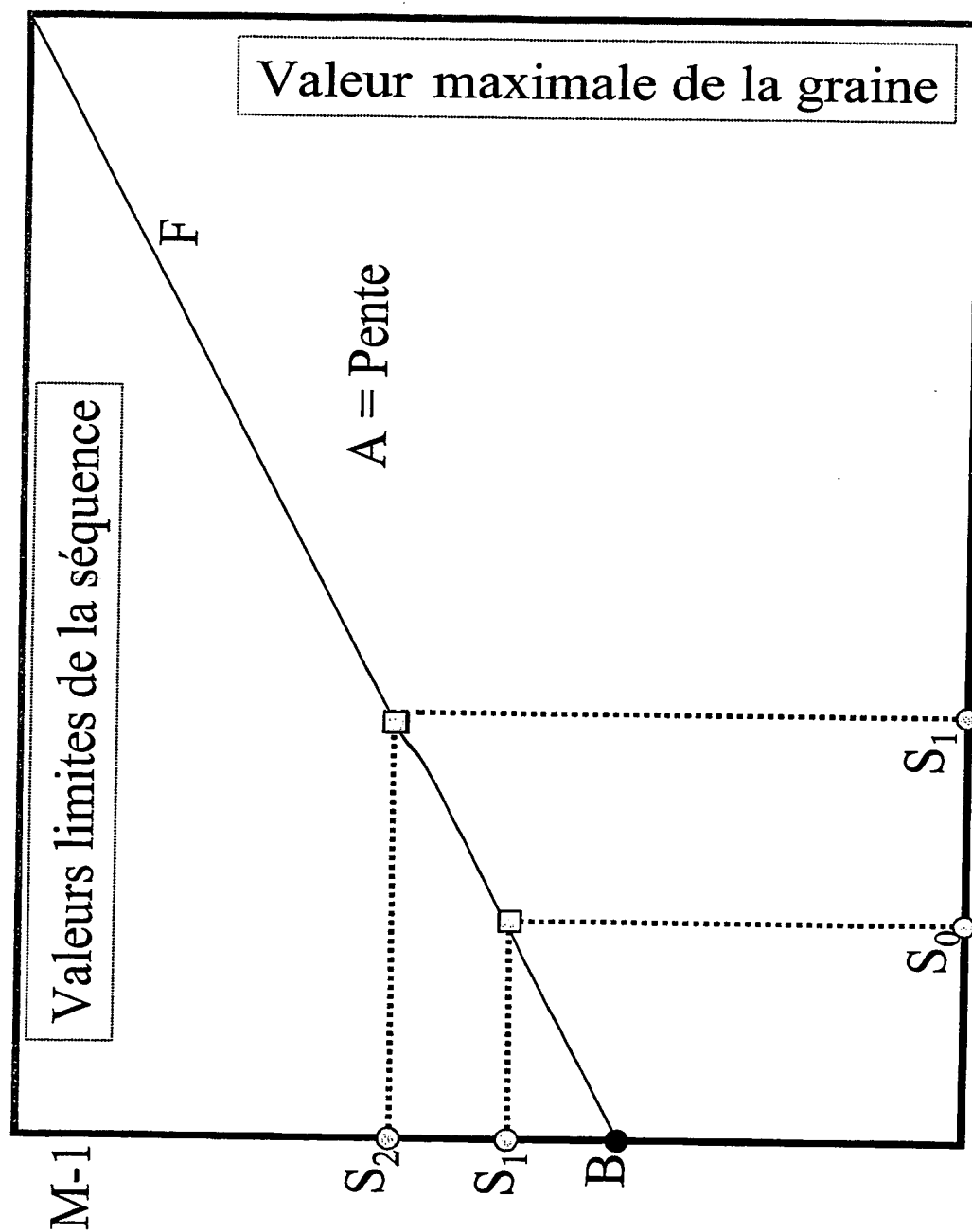
12. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes,
10 caractérisé en ce que lesdites modélisations sont stockées dans une carte à puce de l'équipement destinataire.

13. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes,
15 caractérisé en ce que ladite synthèse du flux d'origine est effectuée en fonctions des paramètres des modélisations, reproduisant les valeurs pseudo-aléatoire obtenues lors des étapes d'analyse.

20 14. Procédé pour la distribution de séquences audiovisuelles selon l'une des revendications précédentes, caractérisé en ce qu'il est sans perte.

15. Système pour la fabrication d'un flux audiovisuel
25 pour la mise en œuvre du procédé selon l'une des revendications précédentes, comportant au moins un serveur multimédia contenant les séquences audiovisuelles originales, caractérisé en ce qu'il comporte un dispositif d'analyse du flux audiovisuel pour la séparation du flux
30 vidéo original en un flux principal modifié et en une information complémentaire en fonction de ladite analyse, au moins un réseau de télécommunication pour la transmission et au moins un dispositif sur l'équipement destinataire pour la reconstruction du flux audiovisuel en fonction dudit flux
35 principal modifié et de ladite information complémentaire.

1/3



M-1

Figure 1



THIS PAGE BLANK (USPTO)

Flux contenant des données aléatoires et pseudo aléatoires

  P D P D P D P D P D P D P D P D

2a

Flux contenant uniquement des données aléatoires

  S D D D D D D D D D

2b




-  Graine qui a généré la séquence pseudo aléatoire, représente une valeur aléatoire
-  Position : donnée pseudo aléatoire
-  Donnée issue d'un flux : donnée aléatoire

Figure 2

THIS PAGE BLANK (USPTO)

3/3

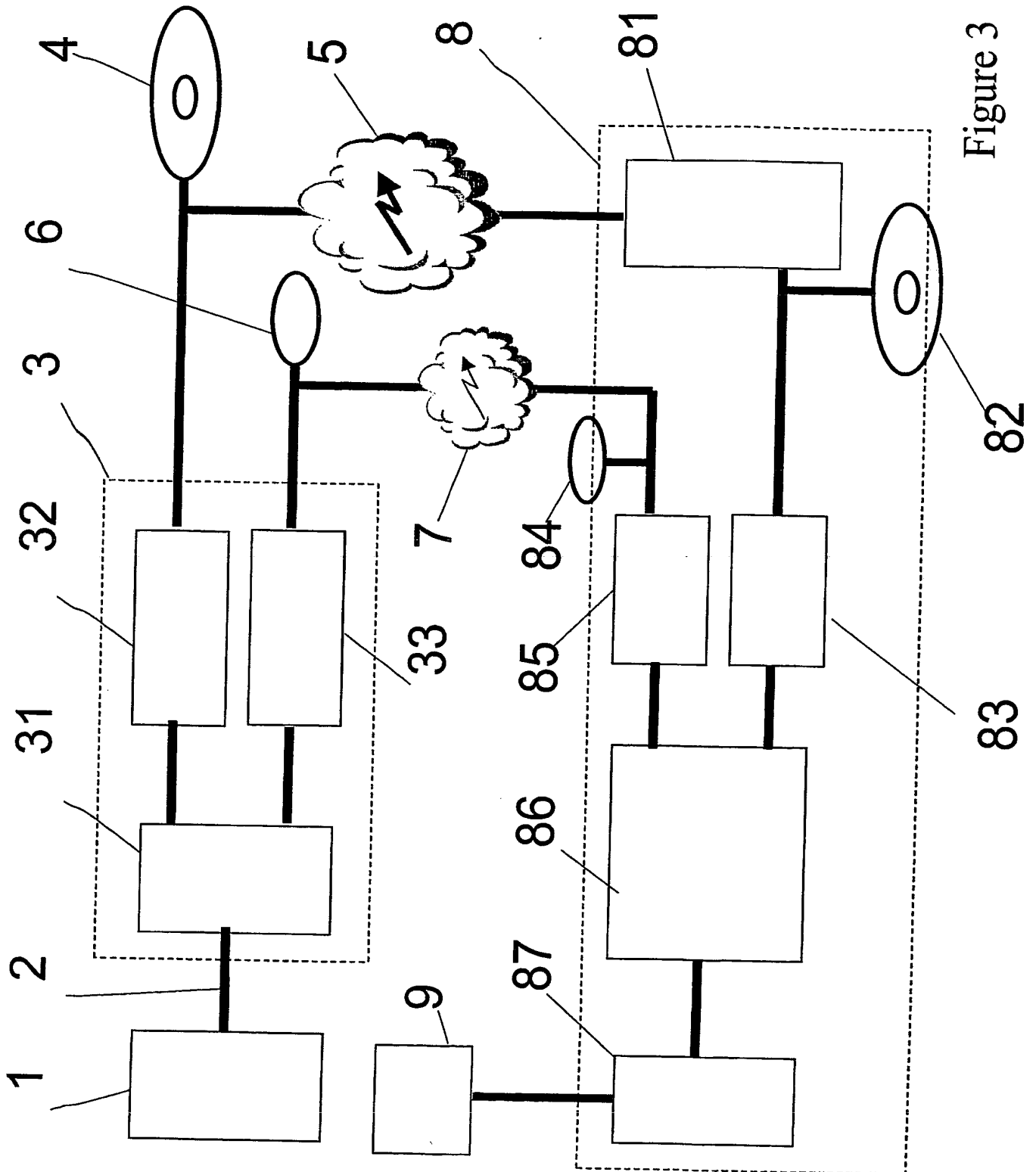


Figure 3

THIS PAGE BLANK (USPTO)